

REMARKS

Claim Rejections – 35 U.S.C. § 103 Over Herrero In View Of Holden

Claims 1-39 stand rejected for obviousness under 35 U.S.C § 103(a) as being unpatentable over Herrero, *et al.*, (WIPO WO 00/74345) (hereafter ‘Herrero’) in view of Holden, *et al.*, (U.S. Patent No. 5,828,832) (hereafter ‘Holden’). The question of whether Applicants claims are obvious or not is examined in light of: (1) the scope and content of the prior art; (2) the differences between the claimed invention and the prior art; (3) the level of ordinary skill in the art; and (4) any relevant secondary considerations, including commercial success, long felt but unsolved needs, and failure of others. *KSR Int’l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1729-1730, 82 USPQ 1385 (2007). Although Applicants recognize that such an inquiry is an expansive and flexible one, the Office Action must nevertheless demonstrate a prima facie case of obviousness to reject Applicants claims under for obviousness under 35 U.S.C. § 103(a). *In re Khan*, 441 F.3d 977, 985-86 (Fed. Cir. 2006). To establish a prima facie case of obviousness, the proposed combination of Herrero and Holden must teach or suggest all of Applicants’ claim limitations. MPEP 2142 (citing *In re Royka*, 490 F.2d 981, 985, 180 USPQ 580, 583 (CCPA 1974)). As shown below in more detail, the proposed combination of Herrero and Holden cannot establish a prima facie case of obviousness because the proposed combination does not teach each and every element of the claims of the present application. As such, Applicants respectfully traverse each rejection individually.

The Proposed Combination Of Herrero And Holden Does Not Teach Or Suggest Each And Every Element Of Claim 1 Of The Present Application

Independent claim 1 of the present application recites:

1. A method for providing a necessary level of security for a computer capable of connecting to different computing environments, the method comprising:

monitoring a type of connection between the computer and a network in a current computing environment;

determining a security level of data before sending the data across the network;

storing the data in a buffer instead of sending the data across the network if the connection to the network lacks a security control required for the determined security level of the data; and

sending the data from the buffer when the computer is connected to a changed computing environment having a new type of connection that has the security control required for the data.

**Herrero Neither Discloses Nor Suggests Monitoring
The Type Of Connection Between A Computer And
A Network In A Current Computing Environment**

The Office Action takes the position that Herrero at page 4, lines 5-10, discloses the first element of claim 1: monitoring the type of connection between a computer and a network in a current computing environment. Applicants respectfully note in response, however, that what Herrero at page 4, lines 5-10, in fact discloses is:

According to an exemplary embodiment of the present invention, these and other objects are met by a method and apparatus for secure communication between entities in one or more networks. A determination is made whether security measures needed for the communication exist between the entities. If such measures do not exist, the security measures are established, and the communication is initiated. The security measures include security bindings including information needed for the secure communication.

That is, Herrero at page 4, lines 5-10, discloses secure communication between entities consisting of determining whether security measures are needed, establishing security

measures if they are needed but do not exist, and initiating communication. Herrero's secure communication between entities does not disclose monitoring the type of connection between a computer and a network in a current computing environment as claimed in the present application. In fact, Herrero does not disclose monitoring at all. Herrero at the cited reference point only discloses determining whether security measures needed for a particular communication exist. Examples of monitoring as claimed in the present application include periodically determining the type of connection between a computer and a network and an event-driven determination of the type of connection between a computer and a network carried out each time the TCP/IP client on a computer runs during the computer's power-up procedure. *See Applicants' Original Specification* at page 15-16. Additionally, Applicants note that at no point in the entire reference does Herrero mention the terms 'monitor' or 'monitoring.' The secure communication between entities consisting of determining whether security measures are needed, establishing security measures if they are needed but do not exist, and initiating communication of Herrero therefore neither discloses nor suggests monitoring the type of connection between a computer and a network in a current computing environment as claimed in the present application. The Office Action therefore cannot establish a prima facie case of obviousness. The rejections under 35 U.S.C. § 103 should be withdrawn, and the claims should be allowed.

**Holden Neither Discloses Nor Suggests Sending Data From
A Buffer When A Computer Is Connected To A Changed
Computing Environment Having A New Type Of
Connection That Has The Security Required For The Data**

The Office Action takes the position that Holden at column 11, lines 50-52, discloses the fourth element of claim 1: sending data from a buffer when a computer is connected to a changed computing environment having a new type of connection that has the security required for the data. Applicants respectfully note in response, however, that what Holden at column 11, lines 50-52 in fact discloses is:

If a write down situation, the SNIU determines if the datagram was predicted and sends or audits the anticipated message as described above. If a write equal, the datagram is released to the destination.

That is, Holden at column 11, lines 50-52, discloses a secure network interface unit (SNIU) that determines if a datagram was predicted and sends or audits an anticipated message. Holden's SNIU that determines if a datagram was predicted and sends or audits an anticipated message does not disclose sending data from a buffer when a computer is connected to a changed computing environment having a new type of connection that has the security required for the data as claimed in the present application. Applicants refer to a group of computers having available to them similar levels of data communications security as a computing environment. *See Applicants' Original Specification*, paragraph 0020, 0072-0073. Holden at the cited reference point, or at any other point, does not disclose a change in any such computing environment. Holden simply discloses the SNIU sending a message based on the receipt of an 'Association grant' message. *See Holden at column 11, lines 30-34.* The SNIU that determines if a datagram was predicted and sends or audits an anticipated message of Holden therefore neither discloses nor suggests sending data from a buffer when a computer is connected to a changed computing environment having a new type of connection that has the security required for the data as claimed in the present application. The Office Action therefore cannot establish a prima facie case of obviousness. The rejections of under 35 U.S.C. § 103 should be withdrawn, and the claims should be allowed.

**The Proposed Combination Of Herrero And Holden
Does Not Teach Or Suggest Each And Every
Element Of Claim 11 Of The Present Application**

Independent claim 11 of the present application recites:

11. A method for providing a necessary level of security for a computer capable of connecting to different computing environments, the method comprising:

connecting the computer to a network in a first computing environment;

specifying a security level for data to be sent across the network;

instructing a sending program to send the data across the network;

receiving an indication that security control of the first computing environment lacks a security control required for the specified security level;

connecting the computer to the network in a second computing environment, wherein the second computing environment has the security control required for the specified security level; and

receiving an indication that the data has been sent across the network.

Herrero Neither Discloses Nor Suggests Connecting A Computer To A Network In A Second Computing Environment, Wherein The Second Computing Environment Has The Security Control Required For A Specified Security Level

The Office Action takes the position that Herrero at page 4, lines 5-20, discloses the fifth element of claim 11: connecting a computer to a network in a second computing environment wherein the second computing environment has the security control required for a specified security level. Applicants respectfully note in response, however, that what Herrero at page 4, lines 5-20, in fact discloses is:

According to an exemplary embodiment of the present invention, these and other objects are met by a method and apparatus for secure communication between entities in one or more networks. A determination is made whether security measures needed for the communication exist between the entities. If such measures do not exist, the security measures are established, and the communication is initiated. The security measures include security bindings including information needed for the secure communication.

Security measures are established between entities in one or more networks based on predetermined security requirements and on a determined needed security level. The security level needed may be determined based on whether the entities are in the same network or in different networks and/or on the information being transmitted. Security bindings are established between the entities depending on the information to be transmitted and/or the network to which the entities belong. The security bindings include information identifying the security binding, encryption information, authentication information, integrity information, a list of addresses or group of addressees included in the security bindings, and/or information regarding the lifetime of the security bindings.

The encryption, authentication, and integrity may be specified at a parameter level.

Applicants have noted previously that Herrero at page 4, lines 5-10, discloses secure communication between entities consisting of determining whether security measures are needed, establishing security measures if they are needed but do not exist, and initiating communication. In addition, Applicants note that what Herrero at page 4, lines 10-20, discloses that these security measures are based on security requirements and security levels, and that security bindings established can include encryption, authentication, and integrity. Herrero's secure communications, security measures, and security bindings do not disclose connecting a computer to a network in a second computing environment wherein the second computing environment has the security control required for a specified security level as claimed in the present application. Herrero's disclosures of secure communications, security measures, and security bindings all require on the computer that wishes to send a message remain on that same network, while the receiving computer can be on another network. *See* Herrero at page 4, lines 12-16. However, at no point in the entire reference does Herrero contemplate the connection of the sending computer to a network in a *second* computing environment, as claimed in the present invention. Herrero only discloses that if security measures do not exist between the sender and receiver, then they are established. The disclosures of Herrero therefore neither disclose nor suggest connecting a computer to a network in a second computing environment wherein the second computing environment has the security control required for a specified security level as claimed in the present application. The Office Action

therefore cannot establish a prima facie case of obviousness. The rejections under 35 U.S.C. § 103 should be withdrawn, and the claims should be allowed.

Relations Among Claims

Independent claims 14 and 24 are system claims for providing a necessary level of security for a computer capable of connecting to different computing environments corresponding to independent claims 1 and 11 that include “means for” providing a necessary level of security for a computer capable of connecting to different computing environments. Independent claims 27 and 37 are computer program product claims for providing a necessary level of security for a computer capable of connecting to different computing environments corresponding to independent claims 1 and 11 that include “means, recorded on [a] recording medium, for” providing a necessary level of security for a computer capable of connecting to different computing environments. For the same reasons that the proposed combination of Herrero and Holden does not disclose or suggest the limitations of claims 1 and 11, the proposed combination of Herrero and Holden also does not disclose or enable systems and computer program products corresponding to independent claims 14, 24, 27, and 37. Independent claims 14, 24, 27, and 37 are therefore patentable and should be allowed.

Dependent claims 2-10 depend from independent claim 1. Dependent claims 12 and 13 depend from independent claim 11. Dependent claims 15-23 depend from independent claim 14. Dependent claims 25 and 26 depend from independent claim 24. Dependent claims 28-36 depend from independent claim 27. Dependent claims 38 and 39 depend from independent claim 37. Each dependent claim includes all the limitations of the independent claim from which it depends. In rejecting dependent claims 2-10, 12, 13, 15-23, 25, 26, 28-36, 38, and 39, the Office Action relies on the combination of Herrero and Holden as disclosing each and every element of independent claims 1, 11, 14, 24, 27, and 37. As shown above, the combination of Herrero and Holden in fact does not disclose each and every element of independent claims 1, 11, 14, 24, 27, and 37. Because the proposed combination of Herrero and Holden does not disclose each and every element of independent claims 1, 11, 14, 24, 27, and 37, the proposed combination of

Herrero and Holden cannot possibly disclose each and every element of dependent claims 2-10, 12, 13, 15-23, 25, 26, 28-36, 38, and 39. The proposed combination of Herrero and Holden, therefore, cannot establish a prima facie case of obviousness, and the rejections of dependent claims 2-10, 12, 13, 15-23, 25, 26, 28-36, 38, and 39 under U.S.C. § 103(a) should also be withdrawn.

**Claim Rejections – 35 U.S.C. § 103
Over Herrero In View Of Ueda**

Claims 1, 14, and 27 also stand rejected for obviousness under 35 U.S.C. § 103(a) as being unpatentable over Herrero in view of Ueda (U.S. Patent No. 5,692,179) (hereafter ‘Ueda’). The question of whether Applicants claims are obvious or not is examined in light of: (1) the scope and content of the prior art; (2) the differences between the claimed invention and the prior art; (3) the level of ordinary skill in the art; and (4) any relevant secondary considerations, including commercial success, long felt but unsolved needs, and failure of others. *KSR Int’l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1729-1730, 82 USPQ 1385 (2007). Although Applicants recognize that such an inquiry is an expansive and flexible one, the Office Action must nevertheless demonstrate a prima facie case of obviousness to reject Applicants claims under for obviousness under 35 U.S.C. § 103(a). *In re Khan*, 441 F.3d 977, 985-86 (Fed. Cir. 2006). To establish a prima facie case of obviousness, the proposed combination of Herrero and Ueda must teach or suggest all of Applicants’ claim limitations. MPEP 2142 (citing *In re Royka*, 490 F.2d 981, 985, 180 USPQ 580, 583 (CCPA 1974)).

**Herrero Neither Discloses Nor Suggests Monitoring
The Type Of Connection Between A Computer And
A Network In A Current Computing Environment**

In finding claims 1, 14, and 27 unpatentable over Herrero in view of Ueda, the Office Action on page 7 states that Herrero at page 4, lines 5-10 discloses the first element of claim 1: monitoring the type of connection between a computer and a network in a current computing environment. However, as previously discussed, Herrero makes no such disclosure. Because Herrero make any such disclosure, it is impossible for the

proposed combination of Herrero and Ueda to disclose or suggest each and every element of claim 1 in the present application. The Office Action therefore cannot establish a prima facie case of obviousness. As such, the rejections under 35 U.S.C. § 103 should be withdrawn, and the claims should be allowed.

**Ueda Neither Discloses Nor Suggests Sending Data From
A Buffer When A Computer Is Connected To A Changed
Computing Environment Having A New Type Of
Connection That Has The Security Required For The Data**

The Office Action takes the position that Ueda at column 4, lines 59-62, discloses the fourth element of claim 1: sending data from a buffer when a computer is connected to a changed computing environment having a new type of connection that has the security required for the data. Applicants respectfully note in response, however, that what Ueda at column 4, lines 59-62 in fact discloses is:

The judging means judges whether the security level of the inquirer and the security level of the retrieved data are in conformity with each other or not. When the security level of the inquirer and the security level of the retrieved data are in conformity with each other, retrieved results of the retrieved data are temporarily stored to the buffer means and are transmitted to a terminal on an inquirer side through the network.

That is, Ueda at column 4, lines 59-62, discloses a security level of the inquirer and the a security level retrieved data. When the security levels are in conformity with each other, Ueda discloses that retrieved results transmitted to a terminal through a network. Ueda's security levels and transmitting results does not disclose sending data from a buffer when a computer is connected to a changed computing environment having a new type of connection that has the security required for the data as claimed in the present application. Applicants refer to a group of computers having available to them similar levels of data communications security as a computing environment. *See Applicants' Original Specification, paragraph 0020, 0072-0073.* Ueda at the cited reference point does not disclose a change in any such computing environment. The cited sections of Ueda therefore neither discloses nor suggests sending data from a buffer when a computer is connected to a changed computing environment having a new type of

connection that has the security required for the data as claimed in the present application. The Office Action therefore cannot establish a prima facie case of obviousness. The rejections of under 35 U.S.C. § 103 should be withdrawn, and the claims should be allowed.

Relations Among Claims

As previously discussed, independent claims 14 and 27 are system and computer program product claims for providing a necessary level of security for a computer capable of connecting to different computing environments corresponding to independent claim 1 that include “means for” and “means, recorded on [a] recording medium, for” providing a necessary level of security for a computer capable of connecting to different computing environments. For the same reasons that the proposed combination of Herrero and Ueda does not disclose or suggest the limitations of claim 1, the proposed combination of Herrero and Ueda also does not disclose or suggest systems and computer program products corresponding to independent claims 14 and 27. Independent claims 14 and 27 are therefore patentable and should be allowed.

The Office Action Does Not Examine The Claims In Light Of The Factual Inquiries Set Forth In *Graham*

In addition to the fact that the Office Action has not established a prima facie case of obviousness, there is at least another reason that the rejections under 35 U.S.C. § 103 should be withdrawn. The Office Action does not examine Applicants’ claims in light of the factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966). As mentioned above, the question of whether Applicants’ claims are obvious *vel non* is examined in light of: (1) the scope and content of the prior art; (2) the differences between the claimed invention and the prior art; (3) the level of ordinary skill in the art; and (4) any relevant secondary considerations, including commercial success, long felt but unsolved needs, and failure of others. *KSR Int’l Co. v. Teleflex Inc.*, No. 04-1350, slip op. at 2 (U.S. April 30, 2007); *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966). “To facilitate review, this analysis should be made explicit.” *KSR*, slip op. at 14

(citing *In re Kahn*, 441 F. 3d 977, 988 (Fed. Cir. 2006)). That is, the Office Action must make explicit an analysis of the factual inquiries set forth in *Graham*. In present case, however, the Office Action does not even mention the factual inquiries set forth in *Graham*. As such, the rejections under 35 U.S.C. § 103 are improper and should be withdrawn.

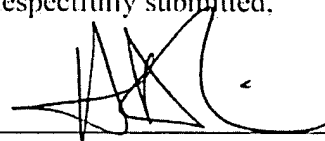
Conclusion

Claims 1-39 stand rejected for obviousness under 35 U.S.C. § 103 as being unpatentable over Herrero in view of Holden. For the reasons set forth above, however, the proposed combination of Herrero and Holden fails to establish a prima face case of obviousness. The rejection of claims 1-39 should therefore be withdrawn, and the claims should be allowed. Reconsideration of claims 1-39 in light of the present remarks is respectfully requested.

Claims 1, 14, and 27 additionally stand rejected for obviousness under 35 U.S.C. § 103 as being unpatentable over Herrero in view of Ueda. For the reasons set forth above, however, the proposed combination of Herrero and Ueda fails to establish a prima facie case of obviousness. The rejection of claims 1, 14, and 27 should therefore be withdrawn, and the claims should be allowed. Reconsideration of claims 1, 14, and 27 in light of the present remarks is respectfully requested.

The Commissioner is hereby authorized to charge or credit Deposit Account No. 09-0447 for any fees required or overpaid.

Respectfully submitted,



Date: April 22, 2008

By:

H. Artoush Ohanian
Reg. No. 46,022
Biggers & Ohanian, LLP
P.O. Box 1469
Austin, Texas 78767-1469
Tel. (512) 472-9881
Fax (512) 472-9887
ATTORNEY FOR APPLICANTS